DATASHEET

CA Agnostic Certificate Lifecycle Management

Sectigo Certificate Manager Works With Multiple Certificate Origins

The average enterprise will need to work with multiple Certificate Authorities (CAs). There are multiple reasons for this - to ensure crypto agility, consolidate existing technology silos, reduce security-stack complexity, enable compliance, and deliver ROI.

Sectigo's market-leading Certificate Lifecycle Management Platform, Sectigo Certificate Manager (SCM), enables the seamless issuance and management of digital certificates originating from private CAs, such as Google Cloud Platform (GCP), AWS Cloud Services and Microsoft Active Directory Certificate Services (ADCS), and publicly trusted CAs. This delivers a robust capability which also includes popular DevOps platforms and leading technology integrations.

This enables CISOs and their teams to discover, deploy, install and renew the lifecycles of all digital certificates deployed within the enterprise ecosystem.

Sectigo's ongoing strategy is built around the trend that cybersecurity leaders are increasingly dissatisfied with the lack of integration within the security stack. As a result, the SCM platform is designed with openness and interoperability at its heart.

Sectigo Automates Certificate Deployment

Sectigo Certificate Manager is CA agnostic, meaning it can work with a host of different IT environments, digital certificate types, use cases, and Certificate Authorities. It automates the issuance and renewal of all digital certificates deployed within an enterprise. SCM achieves this using the latest open standards, without locking customers into a single vendor.

SECTIGO®

How Does This Work?

PUBLIC CA

For public CAs customers are given access to APIs that facilitate the programmatic issuance and renewal of certificates. These APIs require credentials which the CAs provide to their customers. SCM now includes a configurable module for support of third party CAs where the customer can enter their credentials for public CA APIs, providing access to on-demand certificate issuance.

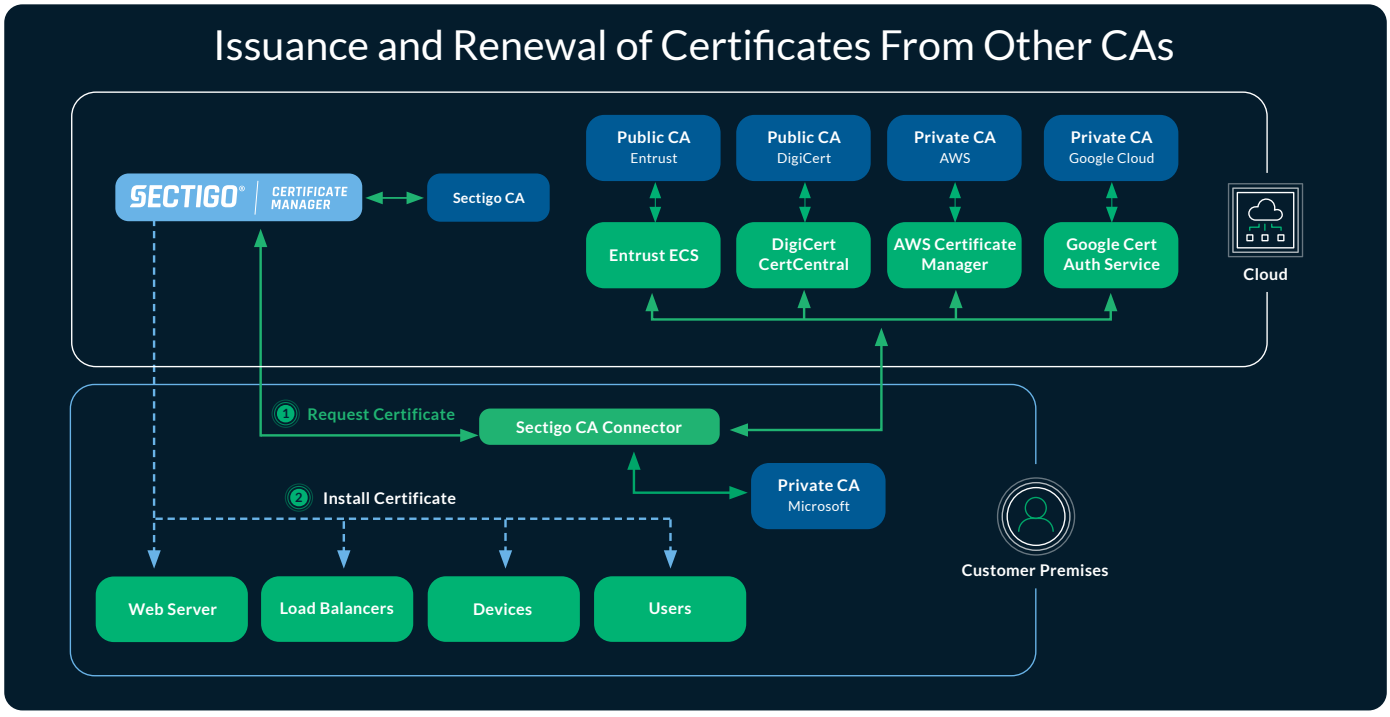
The process for setting up connectivity to a public CA is very straightforward and takes only a few minutes. The API credentials are never shared with Sectigo, and the customer is not required to disclose them. This ensures that Sectigo customers are in full compliance with their contracts with the other CAs.

PRIVATE CA

An enterprise CA, or private CA, is commonly used by businesses to support their authentication infrastructure, internal servers, mobile devices or code and document signing activities. Sectigo provides a private CA as an option with Sectigo Certificate Manager. But many enterprises may already have established Private CAs with Microsoft CA (ADCS), Google Cloud and AWS Cloud. SCM can issue and manage certificates from these CAs, interfacing directly with the vendor's platform. The Sectigo Connector can be configured for multiple instances of these Private CAs, providing complete flexibility and coverage of an enterprise's certificate needs.

CONSOLIDATED PLATFORM

Once the required CAs have been configured, SCM is then used to define a certificate issuance policy with the public or private CA as the source. Requests are issued to the appropriate CA and the certificates can be managed via SCM for installation, renewal, revocation and automation. This provides the customer with the greatest flexibility to continue issuing and renewing certificates sourced from other CAs while managing them via SCM.



Key Benefits of Sectigo Certificate Manager

- **Crypto Agility** - A single pane of glass to manage both public and private certificates issued from Sectigo and other Certificate Authorities.
- **Vendor Consolidation** - An open and easy-to-deploy certificate management solution to avoid platform proliferation and vendor lock-in.
- **Zero-Touch Deployment** - Advanced capabilities to automatically install user and device certificates with a single click.
- **Certificate Management in the Cloud** - Cloud-based efficiency means lower cost of deployment, faster threat discovery, automation, and perimeterless security across cloud and multi-cloud environments.
- **Enterprise Integrations** - Integrations with leading technology providers that give customers deployment flexibility and customizations to work within their unique environments.
- **Dedicated Support** - Industry-leading customer support with white glove service from onboarding to continued account services.

Sectigo's unique approach is both revolutionary and transformative with better alignment with the customer need. SCM provides a modern approach to securing massive amounts of human and machine identities at scale.

For further information on Sectigo's certificate solutions contact your Sectigo sales representative or email sales@sectigo.com.

About Sectigo

Sectigo is the leading provider of digital certificates and automated Certificate Lifecycle Management (CLM) solutions trusted by the world's largest brands. Its cloud-based universal CLM platform issues and manages the lifecycles of digital certificates issued by Sectigo and other Certificate Authorities (CAs) to secure every human and machine identity across the enterprise. With over 20 years of experience establishing digital trust, Sectigo is one of the longest-standing and largest CAs with more than 700,000 customers, including 40% of the Fortune 1000. For more information, visit **www.sectigo.com**.